

Abstract of the Disclosure

Apparatus and an accompanying method, for forming and embedding a highly tamper-resistant cryptographic identifier, i.e., a watermark, within non-marked executable code, e.g., an application program, to generate a "watermarked" version of that code. Specifically, the watermark, containing, e.g., a relatively large number of separate executable routines, is tightly integrated into a flow pattern of non-marked executable code, e.g., an application program, through randomly establishing additional control flows in the executable code and inserting a selected one of the routines along each such flow. Since the flow pattern of the watermark is highly intertwined with the flow pattern of the non-marked code, the watermark is effectively impossible to either remove from the code and/or circumvent. The routines are added in such a manner that the flow pattern of resulting watermarked code is not substantially different from that of the non-marked code, thus frustrating third party detection of the watermark using, e.g., standard flow analysis tools. To enhance tamper-resistance of the watermarked code, each such routine can provide a pre-defined function such that if that routine were to be removed from the marked code by, e.g., a third party adversary, then the marked code will prematurely terminate its execution.